Use of Biometrics in the Virginia Driver's License and Identification Card Process

Karen E. Chappell
Deputy Commissioner
Virginia Department of Motor Vehicles
October 6, 2004

Good afternoon. I am Karen Chappell, Deputy Commissioner for the Department of Motor Vehicles. Thank you for the opportunity to be here to provide information about the agency's efforts to enhance driver's license and identification card security.

DMV is seeking a legislative study on the use of biometrics for state agencies. DMV had planned to develop a legislative proposal seeking the authority to collect and use biometrics in Virginia's driver's license and ID card issuance process.

However, recognizing that the capture and storage of biometric data is a sensitive issue, we respectfully request that an impartial group, such as JCOTS, undertake a study on the use of this technology, not only by DMV but for other state agencies that may also benefit from its use --- such as Virginia State Police, Social Services and the Department of Medical Assistance Services.

There are many critical issues--- from the reliability of available technology to implementation costs to the potential privacy impact--- that a study group will need to evaluate.

Because state-issued driver's licenses and ID cards have become the primary method of identification, it is imperative that we take every possible action to strengthen the issuance process and the integrity of the documents we issue.

We believe the agency needs to use biometrics to help reduce fraud and improve efficiency in the issuance process. The study should include how biometrics can be incorporated into the driver's license issuance process, the types of biometric identifiers and how they are used in other states. I want to highlight each one of these areas.

In a driver's license process, biometrics can function in two ways--- as identification and verification.

As **identification**, an applicant's unique identifier information is used to search an existing database for duplicate data. This is referred to as a one-to-many search, and can help the DMV customer service representative confirm, before issuing the driver's license or ID card, that the customer does not already hold a license or ID.

As **verification**, the information collected can confirm an individual's claimed identity. This is referred to as a one-to-one search--- determining that the fingerprint on file belongs to the cardholder.

There are many types of biometric identifiers. These types include finger or hand scans, handwriting, keyboard ballistics (also called typing rhythms), iris scans and facial recognition. While the agency encourages the study of all available technology, at this time DMV is most interested in using facial recognition and finger scans.

Facial recognition seems to be the least invasive biometric identifier to collect. Facial feature points can be obtained from digital photographs already on file for current license and ID card holders. These applicants would not be asked to submit information that isn't already on file. In addition, facial recognition scans are an efficient and versatile way of addressing identity theft and security issues.

Six states have begun using facial recognition biometrics as a way of using technology to make the license issuance process more secure.

The first facial recognition, or FR, technology among motor vehicle administrations was implemented in West Virginia in 1997. The District of Columbia, Colorado and Illinois are using facial recognition, as well. Alabama and Kansas are in the process of developing FR capabilities.

Colorado's implementation uses facial scanning to eliminate the issuance of duplicate drivers' licenses. As an applicant's digital photo is taken for the license, the photo is immediately searched against the database of other facial images. The technology creates a template of the face by measuring distances between different "landmarks"--- eyes, nose and lips. This template becomes a mathematical formula, unique to each face.

According to the West Virginia DMV, similar technology has prevented the issuance of thousands of duplicate or fraudulent credentials. When renewing a West Virginia license, applicants sign in and are photographed. As photos are taken, the system confirms or denies people's identities by comparing them to their original photos in the database. If the system can't confirm an applicant, a supervisor is called to determine the applicant's identity.

In Illinois, officials use facial recognition technology to search the state's database for duplicate licenses. Illinois reports that it found tens of thousands of duplicates. Some individuals have had as many as a dozen licenses.

While most facial recognition applications prevent the issuance of fraudulent cards, fingerprint technology is usually implemented, such as in Texas, to prevent cards already in circulation from fraudulent use.

With finger scans, the ridges of a fingerprint are converted to minutiae points. To illustrate minutiae points, think of an array of stars in the night sky. Only after focusing on the pattern of a few stars--- connecting the dots--- can you see the Big Dipper. Similarly, using a mathematical formula, minutiae points become a fingerprint template.

Only the template is stored in a database for verification comparisons. And no fingerprint could be recreated with the use of that template.

Fingerprints are required in five states: Texas, California, Colorado, Georgia, and Hawaii. Other states collect fingerprint data on a voluntary basis, including Georgia, Oklahoma, West Virginia and Mississippi.

All states will be using fingerprint technology next year to comply with the federally mandated USA Patriot Act. Effective January 31, 2005, the Act will require individuals applying for a Commercial Driver's License (CDL) with a hazardous materials endorsement to provide specific information and to be fingerprinted for a background check.

To comply, the agency will install electronic fingerprinting equipment at seven DMV locations throughout the state. Applicants will need to visit one of the seven locations to apply for the HAZMAT endorsement and be fingerprinted.

The application information will be entered into the agency's host system and, when fully implemented, transmitted to AAMVA's Commercial Driver's License Information System, known as CDLIS. The Transportation Security Administration (TSA) will retrieve the information from CDLIS and perform name-based checks.

Fingerprints will be sent to the Virginia State Police, utilizing its existing digitized fingerprint protocol for fingerprint submissions to the FBI. Once the fingerprint submission is received from State Police, the FBI will process the transaction and send results to the TSA.

TSA compiles and reviews both sets of data--- the FBI's assessment of the fingerpint and the CDLIS findings about the applicant's name. At the end of the review, TSA makes a security threat assessment and provides DMV with one of four specific actions.

1) Immediate revocation of the applicant's hazardous materials endorsement.

2) Initial Notification of Threat Assessment. This is an initial indication that TSA found something that may warrant the refusal or revocation of the hazardous material endorsement. The individual has the option to appeal the findings or request a waiver by TSA.

3) Final Notification of Threat Assessment: The process has returned indicators that the applicant is a possible security threat. DMV would not issue the hazardous material endorsement or would revoke the hazardous material endorsement depending on the applicant's status. In addition, the applicant either did not request a waiver or appeal, or was denied a waiver or appeal by TSA after the Initial Notification of Threat Assessment.

4) Notification of No Security Threat: TSA has determined that the applicant does not pose a threat and may be issued a hazardous materials endorsement.

Based on the results from TSA, the DMV will either issue a CDL with the hazardous material endorsement or send the applicant notification of the denial by TSA.

As the agency implements this federal mandate for CDLs, we will be evaluating the process and the possibility of expanding it for the state's overall licensing process.

In the meantime, DMV is changing the current process for issuing driver's licenses and ID cards. Replacing over-the-counter issuance with centralized issuance of driver's license and ID cards will further strengthen the security of Virginia credentials.

Using a centralized process, DMV will accept and review customers' applications and conduct required testing at DMV offices. Applicants meeting identity, legal presence, Virginia residency, social security and testing requirements will be issued a receipt. Driver's license applicants can use this receipt as temporary authorization to operate a motor vehicle. Receipts could include the applicant's photograph. DMV will determine how long receipts are valid.

DMV will transmit applicant data to a third party vendor with whom DMV has contracted and established confidentiality standards. The vendor will produce the driver's licenses and ID cards at a central processing point and mail the cards to the customer. DMV employees will not have any capability to issue licenses or ID cards. The agency does not anticipate unreasonably long turn-around times for mailing finished products to customers. Fifteen states--- Alabama, Colorado, California, Kansas, Maine, Massechussetts, Michigan, Minnesota, Montana, New York, Rhode Island, Texas Utah, Washington and Wyoming--- are already using a centralized system and are able to provide products to customers within three to five days.

This type of process is not unfamiliar to Virginians. Customers who take advantage of DMV's web site to renew driver's licenses can use their receipt as proof of renewal until the new driver's license arrives in the mail within a few days.

Central issuance increases security of DMV-issued documents; is similar to the process used to issue U.S. passports; increases customer use of Internet, phone and mail renewal options; and reduces the potential for driver's license and ID card fraud.

As we move forward with central issuance of driver's licenses and ID cards we are planning for the possibility of adding biometrics into the process. The technology could be used as verification at the front counter for those customers renewing driver's licenses or as identification of an applicant before DMV issues an original license or ID card.

In a study of the use of biometrics, heavy emphasis must be given to privacy concerns. Virginia statute (46.2-208) protects DMV customer records and defines the disclosure of privileged DMV records. The definition of "personal information" references the Government Data Collection and Dissemination Practices Act which, includes in the definition, "personal characteristics, such as finger and voice prints." However, a study of biometrics should include a thorough review of existing statutes to identify any changes needed to fully address the public's potential privacy concerns.

In summary, a study should examine available technologies, varying biometric uses, collection and storage of information, the critical importance of data integrity and privacy, costs and implementation strategies, including extensive public outreach and education efforts.

The results of such a study would benefit not only DMV, but also other agencies with a vested interested in this technology. It is important with any new system to balance the benefits and the risks. Ultimately, DMV will take every possible action to strengthen the issuance process and the integrity of the documents we issue. DMV believes that a legislative study--- collecting input from various agencies and organizations--- would greatly assist in the effective implementation of any new program utilizing biometric information.